UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,470	06/13/2001	Radia J. Perlman	P5761	5216

45774 7590 11/14/2005

KUDIRKA & JOBSE, LLP
ONE STATE STREET, SUITE 800
BOSTON, MA 02109

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Supplemental **Notice of Allowability**	Application No. 09/880,470	Applicant(s) PERLMAN, RADIA J.	
	Examiner Peter Poltorak	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an email correspondence from Paul D. Sorkin on 11/03/05*.

2. ☒ The allowed claim(s) is/are *1,4-7,9-23,25-28,30-33,35 and 37*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Supplemental Examiner Amendment

An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the Issue Fee.

The following changes were authorized (and permission to make same by Authorization for this Examiner's Amendment was given in an email correspondence from Paul D. Sorkin on 11/03/05).

Claims 1, 27, 28, 32 and 33 have been amended to clarify the claim language to prevent any possible ambiguity in regard to antecedent basis for all terms contained within the claims.

For example, claim 1, line 4, is amended to refer to a first decryption key corresponding to the first encryption key to provide antecedent basis for subsequent reference to the first decryption key at lines 20-21. The other claims are being similarly amended.

These amendments have not been made to distinguish over any reference of record and no narrowing of any corresponding equivalents to which the amended limitations or claims is/are entitled is intended by these amendments

Examiner Amendment

An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the Issue Fee.

The following changes were authorized (and permission to make same by Authorization for this Examiner's Amendment was given in an email correspondence from Paul D. Sorkin on 11/03/05).

Claims 1, 27, 28, 32 and 33 have been amended to clarify the claim language to prevent any possible ambiguity in regard to antecedent basis for all terms contained within the claims.

For example, claim 1, line 4, is amended to refer to a first decryption key corresponding to the first encryption key to provide antecedent basis for subsequent reference to the first decryption key at lines 20-21. The other claims are being similarly amended.

These amendments have not been made to distinguish over any reference of record and no narrowing of any corresponding equivalents to which the amended limitations or claims is/are entitled is intended by these amendments

Claim 1

--

A method of performing secure ephemeral communication comprising:

receiving, at a first node, a triply wrapped value, said value being encrypted with a first encryption key, having an associated first decryption key, to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

securely communicating said doubly wrapped value to a second node from the first node;

obtaining a second decryption key having a predetermined expiration time at the second node;

determining if said second decryption key has expired;

decrypting said doubly wrapped value using said second decryption key to produce said singly wrapped value if it has been determined that said second decryption key has not expired; and

securely communicating said singly wrapped value from the second node to the first node,

wherein the first and third encryption keys are the same and the first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node.

--

Claim 27

--

A system for performing secure ephemeral communication comprising:

first, second and third communicably coupled nodes, each of said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

program code within said first node memory for receiving a triply wrapped value, said value being encrypted with a first encryption key, having an associated first decryption key, to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value, and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

program code within said first node memory for decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

program code within said first node memory for securely communicating said doubly wrapped value to said second node;

program code within said second node memory for obtaining a second decryption key having a predetermined expiration time at said second node, wherein said second decryption key is associated with said second encryption key;

program code for determining if said second decryption key has expired;

program code within said second node memory for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired; and

program code within said second node memory for securely communicating said singly wrapped value to the first node following decryption of said doubly wrapped value,

wherein said first and third encryption keys are the same and said first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node.

--

Claim 28

--

The system of claim 27 further including program code within said first node memory for decrypting said singly wrapped value using the first decryption key associated with said first encryption key.

--

Claim 32

--

A system for performing secure ephemeral communication comprising:

first, second and third communicably coupled nodes, each of said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

means associated with said first node for receiving a triply wrapped value, said value being encrypted with a first encryption key, having an associated first decryption key, to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value, and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

means associated with said first node for decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

means associated with said first node memory for securely communicating said doubly wrapped value to said second node;

means associated with said second node for obtaining a second decryption key having a predetermined expiration time, wherein said second decryption key is associated with said second encryption key;

means associated with said second node for determining if said second decryption key has expired;

means associated with said second node for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired; and

means associated with said second node memory for securely communicating said singly wrapped value to the first node following decryption of said doubly wrapped value;

wherein said first and third encryption keys are the same and said first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node.

--

Claim 33

--

The system of claim 32 further including means associated with said first node for decrypting said singly wrapped value using the first decryption key associated with said first encryption key.

--

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached from Monday through Thursday from 9:00 until 5:00, and every other Friday from 9:00 until 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-1600.

11/8/05

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100